Cloud Data Storage Security by Applying Modified DNA Cryptography

Ramesh Shah[#1], Ravi Singh Pippal [*2]
[#1]*M.Tech Scholar, Computer Science and Engineering*
[*2]*Professor, Computer Science and Engineering*
Vedica Institute of Technology
RKDF University, Bhopal, India

Abstract: One of the well-known technologies that take care of security of data getting stored in cloud is Cryptography. Applying the concept of digital signature that enables users to validate the proposed document. Modernized & advanced preservation technology with low time consumption in between the process of data file encryption & decryption become possible only due to proposed algorithm.

Keywords: Cloud Computing; Security; Integrity; Confidentiality; Authentication; Digital Signature; DNA Sequencing;

I. INTRODUCTION

Storing area in a network along with the reckoning resources is the contribution of advanced term called as Cloud Computing. For the freely usage of computational resources connection of network is necessary that allows to get connected to cloud. The use of cloud computing benefitted man companies too now a days which uses computational resources through cloud like AMAZON, GOOGLE, AZURE. Also, the term NIST provides various features that are necessary for a favor called as cloud. National Institute of Standards and Technology (NIST) of U.S. has defined cloud computing with two models Delivery Model:]: specified kinds of services that can be freely available with access on cloud enabling with various platforms such as Software-as-a Service(SaaS), Communication-as-a-Service(CaaS), Platform-as-a-Service(PaaS) and Infrastructures-as-a-Service (IaaS). It figures details user's data stored or accessible on cloud can't be altered or modified. Where users' applications are processed with any alternation, medication are called as computational integrity.

To maintain confidentiality is the foremost goal with cloud computing services. Risks involved with such computational method such a Malicious SysAdmin, VM attack through side channels etc. The term says the data must be in access or approach as and when needed by the user in cloud. There can also be vulnerabilities like attacking of flood, Dos etc. The amenability to enable user with respective resources, services, performances per the service level agreement (SLA). Vulnerabilities in such cloud accountability are SLA opposition, incorrect billing of usage of resources.

The main aim of cloud computing is to provide stable, rapid, convenient data storage and virtualized data and computing resources and services over the Internet to meet the computing needs of the user. While cloud computing provides several advantages, it also has many important risks or problems. Here we present categorized security problems with an SPI model (SaaS, PaaS, IaaS).

This paper is arranged as follows. Section II reviews related work of trusted cloud environment with respect to confidentiality, integrity and authenticity while section III describes proposed security methodology. Section IV gives result analysis of proposed security algorithm. Section V concludes with the performance of proposed secure framework with future enhancements.

II. LITERATURE REVIEW

Vikram et al. [1] discussed that the security could not be offered by the conventional cryptographic algorithms that lacks in their security for the huge amount of growing data, which could be easily broken by the intruders for their malicious activities. Improving the security of data housed in cloud storage is proposed by Kumar [2] For encrypting user data, the proposed solution uses the RSA algorithm and the AES algorithm. Before it is processed in the cloud, the hybridization of these two algorithms enables improved data security. Ahmed Albugmi et al. [3] give an examination of cloud data and safety-related aspects. This paper will outline strategies and techniques used worldwide to guarantee optimal data security by reducing threats and risks. Cloud data availability is useful to many applications, but it poses risks by revealing information to applications that might already have a security vulnerability in them.

Gurjeet Singh et al.[4] In this paper, Cloud Computing is the creation and use of computer technology based on the Internet ("cloud") ("computing"). It is a computing pattern wherein, as a service over the Internet, dynamically scalable and sometimes virtualized services are provided. Lynda Kacha et al. [5] offered an overview of cloud computing data protection problems. Its aim is to highlight the key data protection issues posed by the cloud world. The use of computing tools, such as hardware and software, as a service across a network is used by Charanya R & Al.[6] Cloud computing. The device provides remote providers with data and software from a user and allows a user to store a large number of calculations in a large volume.

Hashizume K. Et al [7] suggested that Cloud Computing is a scalable, cost-effective and tested distribution mechanism for the Internet provision of business or consumer IT services. Cloud Computing is a computer and storage facility that helps Aakanksha Singh et al. to minimize investments into computer technology organizations[8]. The challenges to this technology are now more tangible than ever since the cloud computing has been on the increase for many years. In order for industry to be legitimized by the citizen concerned, it must first resolve a range of possible challenges beyond cyber-criminality.

Albugmi A. et al. [9] This paper deals with cloud data protection. It is a cloud analysis of data and security-related aspects. It will outline the strategies and techniques of data protection used globally to ensure the highest standard of data protection by reducing threats and risks. Cloud computing is the technology that enables individuals to share resources, services and information through internet use with people. Lenka S.R et al. [10]. Security is considered to be a major problem because we exchange the data through the internet. Several security problems exist in cloud computing, such as anonymity, honesty and authentication. A new security model has been suggested in this paper.

Meng D et al.[11] This paper addresses issues of cloud computing data protection, including tile data transmission security, storage, security and security management. Namasudra S et al.[12] In the IT industry, cloud computing is a very developing field. Many distributed systems are connected in a cloud environment to provide the internet with software, hardware and resources. Because this new model needs users to protect their personal data, the security and privacy problems with outsourced data are increasingly growing. Priya Lyeret al.[13] One of the growing innovations associated with grid computing, utility computing, distributed computing, is cloud computing. Securing knowledge plays a critical role in today's environment.

III. PROPOSED METHODOLOGY

Cloud computing has been flourishing in past years thanks to its ability to produce users with on-demand, flexible, reliable, and affordable services. Some examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The key reason for the proposal is the safety issue for the privacy as well as the confidentiality of the Server End data file during cloud storage. The proposed work is hybrid in nature, which contains three stages. It is conducted to keep securities at cloud storage following skeleton.

```
Algorithm:
Step 1: Input data
Step 2: Encrypt data using Algorithm given in below section.
Step 3: Divide encrypted data file into blocks of different sizes block size
Step 4: Generate Digital Signature of each block
Step 5: Send the encrypted data blocks to the cloud data server to store these blocks.
Step 6: If user wants to check integrity of stored data or wants to audit data
{
Data owner send request to TPA
Cloud Server sends data blocks to TPA
        TPA generates hash code on these blocks and send the audit report to data owner.
}
Step 7: Exit
```

The work proposed (Fig.1) is made up of three steps. In first stage, digital signature of the data file is generated by the user. This digital signature is generated by using the private key of the user, so that user is authenticated at the server end. After generation of digital signature, the proposed algorithm moves towards the second stage. In second stage user encrypts the data using modified DNA cryptography algorithm. After that the encrypted data hash value is generated by the user and send it to the Third-Party Auditor i.e., TPA. User also sends the encrypted data along with digital signature to the cloud server. This is the completion of second stage and start of third stage of file storage process. In this stage cloud server saves it at the cloud storage server or data center.

DNA Cryptography Binary optical encryption encoded by a combination of two states 0 or 1 and 0 and 1 in information technology The digital DNA coding, however, can be encoded using four forms of database: ADENINE (A) THYMINE (T) or CYTOSINE (C) and GUANINE (G). There are maybe 4! =24 pattern by format encoding. ATGC is being used as a key here in this work. Each bit has 2 bits, such as A=00, T=01, G=10, and C=11, and key combinations are generated and numbered using ATGC.

Further DNA Cryptography is used to re-encrypt the encrypted data file in first level. In information science, the binary digital coding encoded by two state 0 or 1 and a combination of 0 and 1.

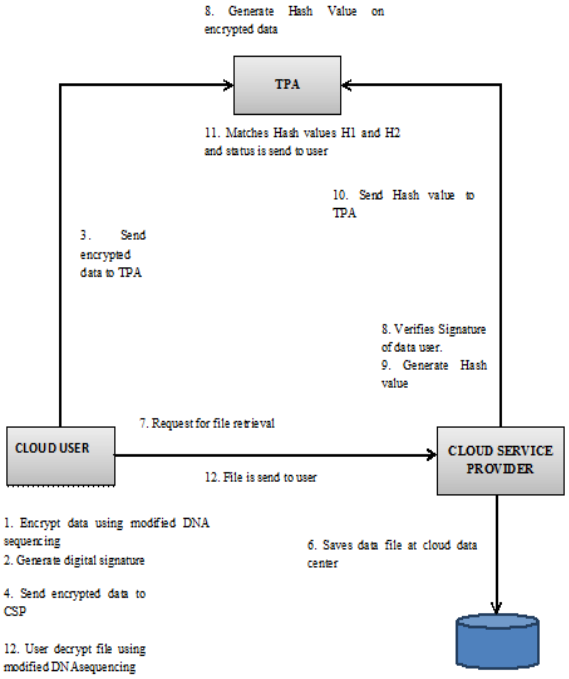
8. Generate Hash Value on encrypted data
TPA
11. Matches Hash values H1 and H2 and status is send to user
10. Send Hash value to TPA
3. Send encrypted data to TPA
8. Verifies Signature of data user.
9. Generate Hash value
7. Request for file retrieval
CLOUD USER
CLOUD SERVICE PROVIDER
12. File is send to user
1. Encrypt data using modified DNA sequencing
2. Generate digital signature
4. Send encrypted data to CSP
12. User decrypt file using modified DNAsequencing
6. Saves data file at cloud data center

Fig.1. Proposed File Storage Methodology

Table 1. DNA Digital Coding

BinaryValue	DNADigitalCoding
00	A
01	T
10	G
11	C

Table 2. DNA Key Combination

Key Combination	Pattern	Value
AA	0000	0
AT	0001	1
AG	0010	2
AC	0011	3
TA	0100	4
TT	0101	5
TG	0110	6
TC	0111	7
GA	1000	8
GT	1001	9
GG	1010	10
GC	1011	11
CA	1100	12
CT	1101	13
CG	1110	14
CC	1111	15

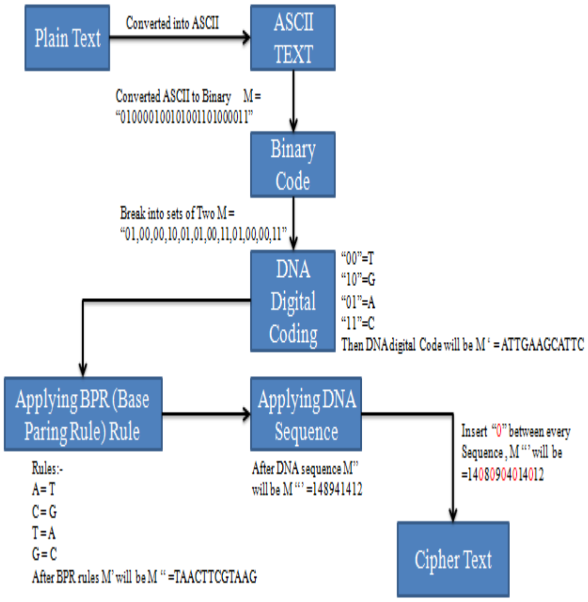
Plain Text
Converted into ASCII
ASCII TEXT
Converted ASCII to Binary M= “010000100101001101000011”
Binary Code
Break into sets of Two M= “01,00,00,10,01,01,00,11,01,00,00,11”
DNA Digital Coding
“00”=T
“10”=G
“01”=A
“11”=C
Then DNA digital Code will be M‘ =ATTGAAGCATTC
Applying BPR (Base Paring Rule) Rule
Rules:-
A=T
C=G
T=A
G=C
After BPR rules M’ will be M “ =TAACTTCGTAAG
Applying DNA Sequence
After DNA sequence M” will be M “‘ =148941412
Insert “0” between every Sequence , M “‘ will be =14080904014012
Cipher Text

Fig.2. DNA Encoding Process

Proposed Encryption Process This algorithm is iterated for 10 rounds. After 10 rounds, the encrypted data is send to DNA algorithm for re-encryption. Detailed steps of encryption process is described below:

Note: PT = Plain Text, K = Key, L = Left part of PT, R = Right part of PT, $^{1}K_{64}$ & $^{2}K_{64}$ = Sub-Keys of K , CT_1 = Cipher Text generated after encryption.

Step 1: Input PT & K

Step 2: Divide PT=L & R

Step 3: Divide K = $^{1}K_{64}$ & $^{2}K_{64}$

Step 4: L>>r→ L (2-bit Right Circular shift)

Step 5: L $\oplus$ R → L (XOR operation)

Step 6: R>>r→ R (2-bit Right Circular shift)

Step 7: Swap L & R

Step 8: L $\oplus$ $^{1}K_{64}$→ L

Step 9: L << l → L (2-bit Left Circular shift)

Step 10: L $\oplus$ R→ R

Step 11: R << l→ R (2-bit Right Circular shift)

Step 12: Swap L & R

Step 13: L $\oplus$ $^{2}K_{64}$→ L

Step 14: Repeat step 4 to 13 up to 10 roundsStep 15: CL + CR = CT_1

For each of the blocks, every element is transformed into an 8-bit binary equivalent, which is then converted into DNA nitrogenous bases.

File recovery process is also called cloud data center decryption. If a user wishes to access a file that is stored at the data center, he first sends an integrity check request to TPA. Before checking integrity of data file cloud server checks the digital signature's validity. If the signature is valid then only it sends to TPA and user for further processing. TPA generates the hash value using SHA algorithm on received encrypted data and matches with the hash value send by the user previously. If hash values matches then TPA sends audit report to the user for further proceedings.

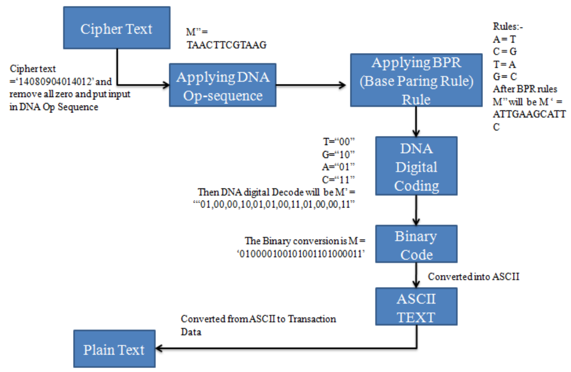

Fig.3. DNA Decoding Process

After decryption through DNA cryptography, proposed decryption module re-decrypt the data file using given below algorithm.

Note: CT_1 = Cipher Text retrieved from database, K = Encrypted Key, CL = Left part of CT_1, CR = Right part of CT_1, $^{1}K_{64}$ & $^{2}K_{64}$ = Sub-Keys of K , PT = Plain Text generated after completion of decryption process of proposed algorithm.

Step 1: Input CT_1 & K

Step 2: Divide CT_1 = CL & CR Step 3: Divide K = $^{1}K_{64}$ & $^{2}K_{64}$

Step 4: CL $\oplus$ $^{2}K_{64}$------------------> CL (XOR operation)

Step 5: Swap CL & CR

Step 6: CR >> R -----------------> CR (2-bit Right circular shift)

Step 7: CL $\oplus$ CR------------------> CR

Step 8: CL >> R------------------> CL (2-bit Right circular shift)

Step 9: CL $\oplus$ $^{1}K_{64}$------------------> CL

Step 10: Swap CL & CR

Step 11: CR <<L------------------> CR (2-bit Left circular shift)

Step 12: CL $\oplus$ CR ----------------- > CR

Step 13: CL << L ----------------- > CL (2-bit Left circular shift)

Step 14: Repeat step 4 to 13 up to 10 roundsStep 15: CL + CR> PT

IV. RESULT ANALYSIS

The experiments are done are done under following system parameters: For implementation of proposed method, following hardware's and software's are required (Minimum requirement) -

Software Tools-Following software were used
Java development kit (like JDK)
Net Beans 7.0 or any above
Operating System (Windows OS)
Simulator Cloud-Sim 3.0

Hardware Tools- Minimum hardware requirements for implementation are as follows-
Hard Disk storage 10 GB or above
RAM 1-GB or above
Processor I-3 and above
Keyboard & Mouse

For evaluation of performance of proposed algorithm the parameters or criteria is to be determined to analyze or test its efficiency. Here the execution time is preferred factors to analyze the performance of the proposed algorithm to encrypt/decrypt data blocks of various sizes.

The total time needed by a data file encryption operation, i.e. convert plain text in cypher text, is called encryption time, or decryption time is called cypher text to plain text. Diverse file size, like 5 KB, 10KB, 15KB up to 50KB, are used to test the execution process. After all data files have been scanned on current techniques, the execution time is decreased as the data file size increases.

Table 3. Total Execution Time Analysis

File Size	Encryption	Decryption
	Execution Time (in ms)	
5KB	2.23	0.93
10 KB	3.21	1.43
15 KB	3.9	1.79
20 KB	4.24	2.90
25KB	4.36	2.90
30KB	4.45	3.51
35KB	4.62	3.97
40KB	4.78	4.98
45KB	4.85	4.11
50KB	4.94	4.82
Average	6.585	2.805

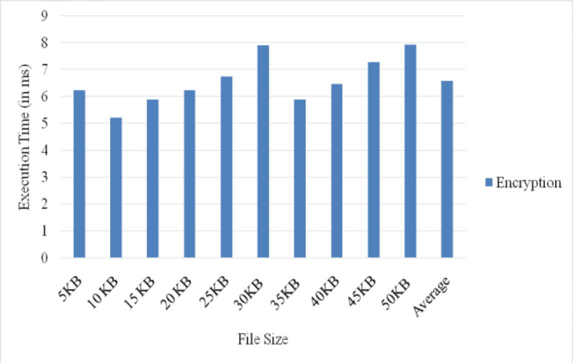

Fig. 4. Encryption Time Analysis

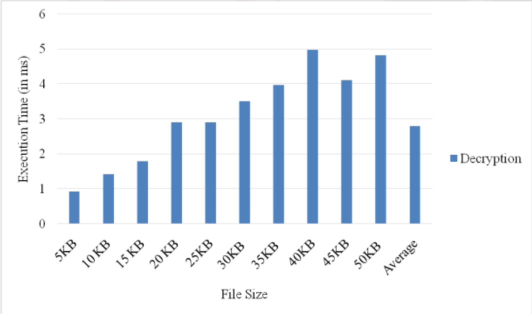

Fig.5. Decryption Time Analysis

Table 4. Total Execution Time Analysis

File Size	Existing [1]	Proposed
	Encryption Time (in ms)	
80KB	6	5.34
100KB	13	6.43
300KB	36	12.56
1000KB	66	23.45
13000KB	76	42.56

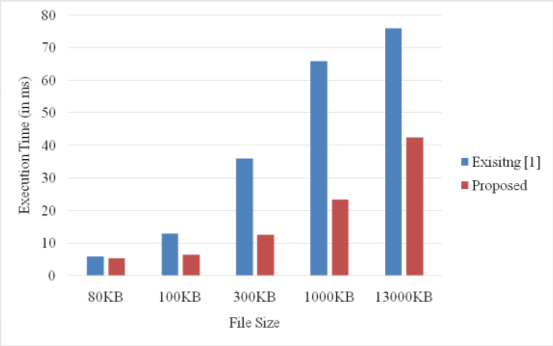

Fig. 6. Comparative Analysis of Encryption Time

Table 5. Total Execution Time Analysis

File Size	Existing [1]	Proposed
	Decryption Time (in ms)	
80KB	16	4.23
100KB	33	12.53
300KB	46	21.54
1000KB	53	36.42
13000KB	66	56.62

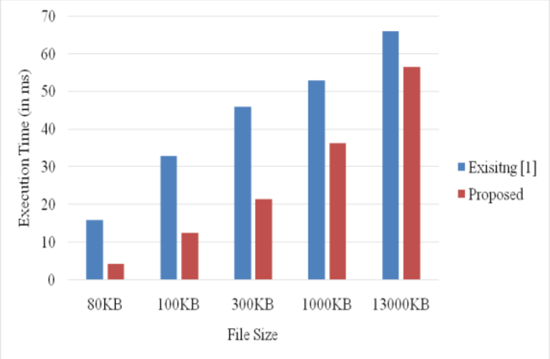

Fig.7. Comparative Analysis of Decryption Time

V. CONCLUSION

The proposed work maintains confidentiality, integrity and authenticity in the cloud environment. Authenticity is maintained by Digital signature algorithm. For confidentiality maintenance hybrid encryption algorithm based on modified DNA cryptography is proposed. Last but not the least, for integrity maintenance SHA algorithm is used by the

TPA on encrypted data file. The experimental results presented show that the proposed idea is rational and that it can increase performance time quality, such as encryption, decryption time and protection as well as confidentiality of cloud data. A framework to process safe data sharing between various cloud users could be a future addition to the method. The proposed method gives a secure framework for verifying the integrity of information files on cloud storage records that can be beneficial for various applications at the cloud server. The proposed algorithm is designed in such a way that it is simple as well as efficient in terms of confidentiality and security. A future enhancement of this proposed algorithm is to batch process different user jobs as well secure sharing data files among different users and to check integrity at cloud server.

REFERENCES

[1] A. Vikram, S. Kalaivani and G. Gopinath, "A Novel Encryption Algorithm based on DNA Cryptography," 2019 International Conference on Communication and Electronics Systems (ICCES), 2019, pp. 1004-1009, doi: 10.1109/ICCES45898.2019.9002399.

[2] A. Kumar, "A Novel Privacy Preserving HMAC Algorithm Based on Homomorphic Encryption and Auditing for Cloud," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2020, pp. 198-202, doi: 10.1109/I-SMAC49090.2020.9243340.

[3] Ahmed Albugmi, Madini O. Alassafi “Data Security in Cloud Computing”, Conference: 2016 Fifth International Conference on Future Generation Communication Technologies (FGCT), IEEE,At: Luton, UK Volume: 1, August 2016. DOI: 10.1109/FGCT.2016.7605062.

[4] Gurjeet Singh, Dr. Mohita Garg “Data Security In Cloud Computing: A Review” July 2018INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY 17(2):7206-7214 DOI: 10.24297/ijct.v17i2.7551

[5] Lynda Kacha, Abdelhafid Zitouni “An Overview on Data Security in Cloud Computing” Conference: Proceedings of the Computational Methods in Systems and Software, DOI: 10.1007/978-3-319-67618-0_23, September 2018.

[6] Charanya R., Aramudhan, M.: Survey on access control issues in cloud computing. In: IEEEInternational Conference on Emerging Trends in Engineering, Technology and Science, pp. 1–4. IEEE (2016).

[7] Hashizume, K., Rosado, D.G., Fernández-Medina, E., Fernandez, E.B.: An analysis of security issues for cloud computing. J. Internet Serv. Appl. 4, 5 (2013).

[8] Aakanksha Singh “An Analysis of Security Issues and Solutions for Cloud Computing”, International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181, Vol. 4 Issue 02, February-2015

[9] Albugmi, A.A., Alassafi, M.O., Walters, R., Wills, G.: Data security in cloud computing. In:,IEEE Fifth International Conference on Future Generation Communication Technologies,pp. 55–59. IEEE (2016).

[10] Lenka, S.R., Nayak, B.: Enhancing data security in cloud computing using RSA encryption and MD5 algorithm. Int. J. Comput. Sci. Trends Technol. 2(2014). 2347-8578.

[11] Meng, D.: Data security in cloud computing. In: IEEE International Conference on Computer Science & Education, pp. 810–813. IEEE (2013)

[12] Namasudra S., Roy, P.: Secure and efficient data access control in cloud computing environment: a survey. J. Multiagent Grid Syst. 12,69–90 (2016).

[13] Priya Lyer, K.B., Manisha, R., Subhashree, R., Vedhavalli, K.: Analysis of data security in cloud computing. In: IEEE International Conference on Communication and Bio-InformaticsAdvances in Electrical, Electronics, Information, pp. 540–543. IEEE (2016).